INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Fog computing: Mitigating insider data theft attacks in the cloud

Ankit Choudhary
choudharyac79@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Tushar Nikam
tusharnik@live.com
Terna Engineering College, Navi Mumbai, Maharashtra

Rajkumar Singh
singh.raj110863@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Yogita Kawle
yogitakawle23@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Abhijit Tambe
abhijittambe6993@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

ABSTRACT

Cloud computing guarantees to considerably amendment the manner we tend to use computers and access and store our personal and business data. With this new computing and communications, paradigms arise new information security challenges. Existing information protection mechanisms like secret writing have unsuccessful in preventing information larceny attacks, particularly those perpetrated by the associate degree business executive to the cloud supplier. We tend to propose a special approach for securing information within the cloud victimization offensive decoy technology. We tend to monitor information access within the cloud and observe abnormal information access patterns. Once unauthorized access is suspected and so verified victimization challenge queries, we tend to launch a misinformation attack by returning giant amounts of decoy data to the assailant. This protects against the misuse of the user's real information. Experiments conducted in a very native file setting offer proof that this approach might offer unprecedented levels of user information security in a very Cloud atmosphere.

Keywords: *Cloud computing, Security, User profiling behavior, Decoy technology.*

1. INTRODUCTION

Businesses, particularly start-ups, little and medium businesses (SMBs), square measure more and more choosing outsourcing knowledge and computation to the Cloud. This clearly supports higher operational potency, however, comes with larger risks, maybe the foremost serious of that square measure knowledge larceny attacks. Knowledge larceny attacks square measure amplified if the assaulter may be a malicious business executive. This can be thought of collectively of the highest threats to cloud computing by the Cloud Security Alliance [1]. Whereas most Cloud computing customers square measure well-aware of this threat, they're left solely with trusting the service supplier once it involves protective their knowledge. The shortage of transparency into, in addition to management over, the Cloud provider's authentication, authorization, and audit controls solely exacerbate this threat. The Twitter incident is one example of a knowledge larceny at-tack from the Cloud. many Twitter company and private documents were ex-filtrated to technological web site TechCrunch [2], [3], and customers' accounts, together with the account of U.S. President Barack Obama, were lawlessly accessed [4], [5]. The assaulter used a Twitter administrator's countersign to achieve access to Twitter's company documents, hosted on Google's infrastructure as Google Docs. The injury was vital each for Twitter and for its customers. Whereas this explicit attack was launched by associate degree outsider, stealing a customer's admin passwords is way easier if perpetrated by a malicious business executive. Rocha and Correia define however simple passwords is also taken by a malicious business executive of the Cloud service supplier [6]. The authors conjointly incontestable however Cloud customers' personal keys can be taken, and the way their confidential knowledge can be extracted from a tough disk. once stealing a customer's countersign and personal key, the malicious business executive get access to any or all client knowledge, whereas the client has no suggests that of detective work this unauthorized access. the abundant analysis in Cloud computing security has centered on ways in which of preventing unauthorized and illegitimate access to knowledge by developing refined access management and secret writing mechanisms. However, these mechanisms haven't been able to forestall knowledge compromise. Encryption, typically acclaimed

because the answer to such threats isn't a comfortable knowledge protection mechanism once used alone [7]. We tend to propose a totally completely different approach to securing the cloud mistreatment decoy info technology, that we've come back to decision Fog computing. We tend to use this technology to launch misinformation attacks against malicious insiders, preventing them from distinctive the $64000 sensitive client knowledge from pretending manky knowledge. During this paper, we tend to propose 2 ways in which of mistreatment Fog computing to forestall attacks like the Twitter attack, by deploying decoy info at intervals the Cloud by the Cloud service client and at intervals personal on-line social networking profiles by individual users.

2. SECURING FOG WITH CLOUD

Numerous proposals for cloud-based services describe strategies to store documents, files, and media in an exceedingly remote service might which will that will} be accessed where a user may hook up with the net. a very vexing downside before such services square measure broadly speaking accepted issues guarantees for securing a user's information in an exceeding manner wherever that guarantees solely the user and nobody else will gain access thereto information. {the downside the matter} of providing security of tip remains a core security problem that, to date, has not provided the degree of assurance the majority need. several proposals are created to secure remote information within the Cloud victimization coding and normal access controls. it's honest to mention all of the quality approaches are incontestable to fail from time to time for a spread of reasons, together with in-sider attacks, misconfigured services, faulty implementations, buggy code, and therefore the artistic construction of effective and complicated attacks not unreal by the implementers of security procedures [8]. Building a trustworthy cloud computing surroundings isn't enough, as a result of accidents still happen, and once they do, and knowledge gets lost, there are no thanks to twig back. One has to steel oneself against such accidents. the essential plan is that we will limit the injury of purloined information if we have a tendency to decrease the worth of that purloined data to the offender. we will bring home the bacon this through a 'preventive' misinformation attack. we have a tendency to posit that secure Cloud services may be enforced given 2 extra security features:

2.1 User Behavior Profiling: it's expected that access to a user's data within the Cloud can exhibit a traditional means that of access. User identification may be a well-known technique which will be applied here to model, however, when and the way a lot of a user accesses their data within the Cloud. Such 'normal user' behavior may be ceaselessly checked to work out whether or not abnormal access to a user's data is happening. This methodology of behavior-based security is usually employed in fraud detection applications. Such profiles would naturally embrace volumetrically data, what percentage documents square measure generally scan and the way typically. These easy user-specific options will serve to find abnormal Cloud access based mostly partly upon the dimensions and scope of knowledge transferred [9].

2.2 Decoys: Decoy data, like decoy documents, honey files, honeypots, and varied alternative counterfeit data may be generated on demand and function a way of police work unauthorized access to data and to 'poison' the thief's ex-filtrated data. Serving decoys can confound and confuse a somebody into the basic cognitive process they need ex-filtrated helpful data, once they haven't. This technology could also be integrated with user behavior identification technology to secure a user's data within the Cloud. Whenever abnormal access to a cloud service is detected, decoy data could also be coming from the Cloud and delivered in such the simplest way on seem fully legitimate and traditional. truth user, United Nations agency is that the owner of the knowledge, would without delay determine once decoy data is being come by the Cloud, and thence might alter the Cloud's responses through a spread of means that, like challenge queries, to tell the Cloud security system that it's inaccurately detected AN unauthorized access. Within the case wherever the access is properly known as AN unauthorized access, the Cloud security system would deliver limitless amounts of counterfeit data to the somebody, so securing the user's true information from unauthorized speech act. The decoys, then, serve 2 purposes: (1) confirmative whether or not information access is allowed once abnormal data access is detected, and (2) confusing the offender with counterfeit data. We have a tendency to posit that the mixture of those 2 security measures can offer unexampled levels of security for the Cloud. No current Cloud security mechanism is out there that has this level of security. we've applied these ideas to find illegitimate information access to information hold on an area filing system by intruders, i.e. attackers United Nations agency impersonate legitimate users once stealing their credentials. One might take into account illegitimate access to Cloud information by a scoundrel corporate executive because of the malicious act of a masquerade. Our experimental ends up in an area filing system setting show that combining each technique will yield higher detection results and our results counsel that this approach may fit in some exceedingly Cloud surroundings because the Cloud is meant to be as clear to the user as an area filing system. Within the following, we have a tendency to review shortly a number of the experimental results achieved by victimization this approach to find masquerade activity in an exceedingly native file setting.

A. Combining User Behavior identification and Decoy Technology for entrant Detection

2.3 User Behavior Profiling:

Legitimate users of an ADPS square measure aware of the files thereon system and wherever they're set. Any look for specific files is probably going to be targeted and restricted. AN entrant, however, United Nations agency gets access to the victim's system illegitimately, is unlikely to be aware of the structure and contents of the filing system. Their search is probably going to be widespread and untargeted. supported this key assumption, we have a tendency to profiled user search behavior and developed user models trained with a one-class modeling technique, particularly one-class support vector machines. The importance of victimization one-class modeling stems from the flexibility of building a classifier while not having to share information with completely different users. The privacy of the user and their information is thus preserved. we have a tendency to monitor for abnormal search behaviors that exhibit deviations from the user baseline. in line with our assumption, such deviations signal a possible intruders attack. Our previous experiments valid our assumption and incontestable that we have a tendency to might dependably find all simulated masquerade attacks victimization this approach with an awfully low false positive rate of one.12.

2.4 Decoy Technology:

We placed traps at intervals the filing system. The traps square measure decoy files downloaded from a Fog computing website, an automatic service that provides many forms of decoy documents like return forms, medical records, MasterCard statements, e-bay receipts, etc. [10]. The decoy files square measure downloaded by the legitimate user and placed in highly-conspicuous locations that aren't doubtless to cause any interference with the traditional user activities on the system. A masquerade, United Nations agency isn't aware of the filing system and its contents is probably going to access these decoy files, if he or she is in look for sensitive data, like the bait data embedded in these decoy files. Therefore, watching access to the decoy files ought to signal intruder's activity on the system. The decoy documents carry a Keyed-Hash Message Authentication Code (HMAC) that is hidden within the header section of the document. The HMAC is computed over the file's contents employing a key distinctive to every user. Once a decoy document is loaded into memory, we have a tendency to verify whether or not the document may be a decoy document by computing an HMAC supported all the contents of that document. We have a tendency to compare it with HMAC embedded at intervals the document. If the 2 HMACs match, the document is deemed a decoy and an alert is issued.

The advantages of inserting decoys in an exceedingly filing system square measure three-fold:

(1) The detection of masquerade activity
(2) The confusion of the offender and therefore the extra prices incurred to tell apart real from counterfeit data, and
(3) The deterrence result that, though laborious to live, plays a big role in preventing masquerade activity by risk-averse attackers.
3) Combining the 2 Techniques: The correlation of search behavior anomaly detection with trap-based decoy files ought to offer stronger proof of misconduct, and so improve a detector's accuracy. We have a tendency to expect that police work abnormal search operations performed before AN unsuspecting user gap a decoy file can corroborate the suspicion that the user is so impersonating another victim user. This state of affairs covers the threat model of illegitimate access to Cloud information. Moreover, AN accidental gap of a decoy file by a legitimate user may be recognized as AN accident if the search behavior isn't deemed abnormal. In alternative words, police work abnormal search and decoy traps along might build an awfully effective masquerade detection system. Combining the 2 techniques improves detection accuracy.

We use decoys as AN oracle for confirmative the alerts issued by the device watching the user's file search and access behavior. In our experiments, we have a tendency to do generate the decoys on demand at the time of detection once the alert was issued. Instead, we have a tendency to create positive that the decoys were conspicuous enough for the offender to access them if they were so making an attempt to steal data by inserting them in extremely conspicuous directories and by giving them attractive names. With this approach, we have a tendency to be able to improve the accuracy of our detector. Crafting the decoys on demand improves the accuracy of the detector even additional. Combining the 2 techniques, ANd having the decoy documents act as an oracle for our detector once abnormal user behavior is detected might lower the general false positive rate of the detector. The results of our experiments counsel that user profiles square measure correct enough to find unauthorized Cloud access. once such unauthorized access is detected, one will respond by presenting the user with the prefer or with a decoy document to validate whether or not the access was so unauthorized, the same as however, we have a tendency to used decoys in an exceedingly native file setting, to validate the alerts issued by the anomaly detector that monitors user file search and access behavior.

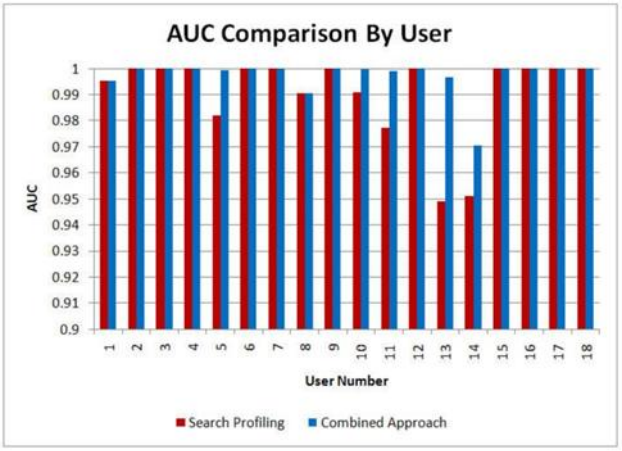

Fig.1. AUC Comparison by User Model for the Search Profiling and Integrated Approaches

3. LITERATURE SURVEY

1) Kaufman L. et al. (2009) has examined some security issues and the associated regulatory and legal concerns that have arisen as cloud computing. Interestingly, a major concern included in the Security Content Automation Protocol is the lack of interoperability between system-level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, we can effectively address cloud computing's future security needs. They also emphasize on the of providing data confidentiality which can impact the incident reporting.

2) Grobauer B. Et al. (2012), provided an overview of vulnerabilities in the security of the cloud. They explained the meaning of the term vulnerability that it it's the probability that an asset is unable to defend itself against a threat. They said vulnerabilities should always be defined in terms of resistance to attacks or threat. Control challenges typically highlight situations in which

otherwise successful security controls are ineffective in a cloud setting. They have discussed the core cloud computing technologies such as web applications and services which use SaaS and PaaS platforms, virtualization and said that there are many such security requirements which are solvable only with the help of cryptographic techniques. Thus, these challenges are of special interest for further cloud computing security research.

3) Sabahi, F. (2011) mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In this paper, he has summarized reliability and availability related issues of cloud resources provided by the trusted third party. He discussed the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown. He said that security is the most argued concern in cloud computing because user's entire data is stored at a remote location and that location needs to be secure enough that it could deal with data thefts and malicious intruders.

4) Claycomb, W. R. (2012) has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers breach the security. They have also presented two additional cloud-related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

5) Park, Y. Et al. (2012) developed a technique that was a software decoy for securing cloud data using the software. They proposed a software-based decoy system that aims to deceive insiders, to detect the exfiltration of proprietary source code. The system builds a Java code which appears as valuable information to the attacker. Further static obfuscation technique is used to generate and transform original software. Bogus programs are synthesized by software that is automatically transformed from original source code but designed to be dissimilar to the original. This deception technique confuses the insider and also obfuscation helps the secure data by hiding it and making bogus information for insider. Beacons are also injected into the bogus software to detect the exfiltration and to make an alert if the decoy software is touched, compiled or executed.

6) Salvatore J. Stoflio et al. proposed a new technique and named it as Fog computing. They implemented security by using decoy information technology. They discussed two methods, namely User behavior profiling, and Decoy. In User behavior profiling they checked how, when and how much amount of information a user is accessing. They monitored their user's activity to check for any abnormality in the data access behavior of the user. The second technology is a decoy in which information which is bogus or we can say fake such as honey files, honey pots, etc. are used to confuse the attacker or malicious intruder by depicting the information in such a way that it seems real. Madsen .H and Albeanu. G presented the challenges faced by current computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real-life projects. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one. A multi-tier architecture is followed in Fog computing platforms. In the first tire, there is a machine to machine communication and the higher tiers deal with visualization and reporting.

4. EXISTING SYSTEM

The existing mechanisms only facilitate security features to data and thereby don't allow for detection of invalid access and thereby its prevention to enable valid distribution of data.

4.1 Disadvantages of Existing System

- Existing data protection mechanisms such as encryption were failed in securing the data from the attackers.
- It does not verify whether the user was authorized or not.
- Cloud computing security does not focus on ways to secure the data from unauthorized access

5. PROPOSED SYSTEM

The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access and thereby its prevention to enable valid distribution of data.

5.1 Advantages of Proposed System

- Fog can be distinguished from Cloud by its proximity to end-users. The dense geographical distribution and its support for mobility.
- It provides low latency, location awareness, and improves quality-of-services (QoS) and real-time applications.

6. IMPLEMENTATION

HARDWARE REQUIREMENTS

- Process: Intel core i3
- Hard Disk: 500GB.
- Ram: 4GB

SOFTWARE REQUIREMENTS

- Operating system: Windows 7/8/8.1/10
- Front End: Visual Basic 2014 ASP.NET
- Back end: SQL2012

SCREEN SHOTS

Figure 1: Home Page

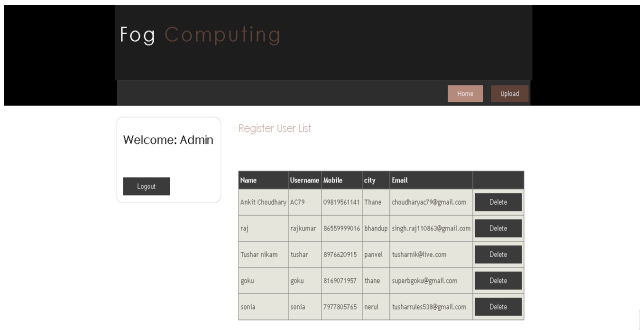

Figure 2: Admin Panel

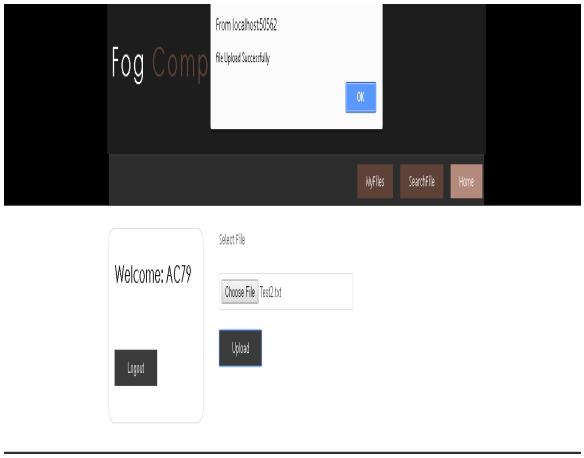

Figure 3: Files Uploaded Successfully

7. CONCLUSION

In this position paper, we tend to gift a completely unique approach to securing personal and business knowledge within the Cloud. We tend to propose observation knowledge access patterns by identification user behavior to work out if and once a malicious business executive illegitimately accesses someone's documents in an exceedingly Cloud service. Decoy documents keep within the Cloud aboard the user's real knowledge conjointly function sensors to discover illegitimate access. Once unauthorized knowledge access or exposure is suspected, and later verified, with challenge queries as an example, we tend to inundate the

malicious business executive with phone info so as to dilute the user's real knowledge. Such preventive attacks that suppose misinformation technology, may offer unexampled levels of security within the Cloud and in the social network.

8. REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March2010. [Online]. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July2009. [Online]. Available:http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/

[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted, "March 2010. Online Available: http://venturebeat.com/2010/03/24/french-hacker-who-leaked-twitter-documents-to-techcrunch-is-busted/

[4] D. Danchev, "ZDNET: French hacker gains access to twitter's admin panel," April 2009. Online Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-to-twitters-admin-panel/3292

[5] P. Allen, "Obama's Twitter password revealed after French hacker arrested for breaking into U.S. president's account," March 2010. Online Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html.

